IN THE CLAIMS:

Please amend claims 1-14 and 16-20, and add new claims 21-28 as follows:

1. (Currently Amended) A storage medium data protecting method of protecting data on a storage medium having a plurality of unit storage areas, comprising:

a step of generating a random key ~~data~~, encrypting ~~the~~ said random key ~~data~~ with a password, and writing ~~the~~ said encrypted random key ~~data~~ to ~~said~~ the storage medium;

a step of encrypting the data with the generated random key ~~data~~, and writing the encrypted data to ~~said~~ the storage medium;

a step of reading ~~the~~ said encrypted key ~~data~~ from ~~said~~ the storage medium;

a step of decoding ~~the~~ said encrypted key ~~data~~ with ~~the~~ said password; and

a step of reading and decoding the data on ~~said~~ the storage medium with the decoded key ~~data~~,

wherein said random key ~~data~~ generating step comprises:

a step of generating a different random key ~~data~~ for each ~~of a plurality of~~ unit storage area of the plurality of unit storage areas ~~of said storage medium~~, so that said each unit storage area is assigned a different random key, and said assignment of said different random key to said each unit storage area being based on a particular unit storage area to which the data, once encrypted, is to be stored;

a step of encrypting each ~~said~~ of the different random ~~key data for each unit storage area~~ keys with said password, and

a step of writing each ~~said~~ of the encrypted ~~key data to said~~ different random keys to the storage medium when initializing the storage medium,

wherein said data encrypting step comprises a step of encrypting the data with ~~the~~ said different random key ~~data~~ corresponding to its said particular unit storage area to write the data, and

wherein said data decoding step comprises a step of decoding the data with ~~the~~ said decoded key ~~data~~ corresponding to said particular unit storage area where the data have been read.

2. (Currently Amended) A storage medium data protecting method according to claim 1, wherein said random key ~~data~~ generating step comprises a step of generating ~~the~~ said random key ~~data~~ per logic sector on ~~said~~ the storage medium.

3. (Currently Amended) A storage medium data protecting method according to claim 1, wherein said random key ~~data~~ generating step comprises a step of generating ~~is~~ different ~~key data~~ random keys for each writing to said plurality of unit storage areas.

4. (Currently Amended) A storage medium data protecting method according to claim 1, wherein said random key ~~data~~ generating step comprises a step of generating ~~the key data~~ said random keys by combining a predetermined number of pieces of random data.

5. (Currently Amended) A storage medium data protecting method according to claim 1, further comprising:

a step of decoding, after reading ~~the~~ said encrypted key ~~data~~ from ~~said~~ the storage medium, ~~the~~ said encrypted ~~key~~ data with an old password designated by a user; and

a step of writing, after encrypting ~~the~~ said decoded key ~~data~~ with a new password designated by ~~the~~ said user, the encrypted ~~key~~ data to ~~said~~ the storage medium.

6. (Currently Amended) A storage medium data protecting method according to claim 1, wherein said ~~step of~~ writing ~~the~~ said encrypted random key ~~data~~ to ~~said~~ the storage medium comprises a step of encrypting ~~the~~ said random key ~~data~~ with each of a plurality of passwords, and writing ~~the~~ said encrypted random ~~key data~~ keys to ~~said~~ the storage medium, and said step of decoding the encrypted key ~~data~~ comprises a step of decoding ~~the read/encrypted data~~said encrypted key with a ~~password~~ designated password.

7. (Currently Amended) A storage medium data protecting method according to claim 1, wherein said ~~step of~~ writing ~~the~~ said encrypted random key ~~data~~ to ~~said~~ the storage medium comprises a step of encrypting ~~the~~ said random key ~~data~~ with a first password, writing the encrypted random key ~~data~~ to ~~said~~ the storage medium, encrypting said first password with a second password, and writing ~~said first~~ the encrypted first password to the storage medium, and said step of decoding the encrypted key ~~data~~ comprises a step of decoding said ~~first~~ encrypted first password with said second password, and obtaining said first password, and a step of decoding ~~the~~ said encrypted key ~~data~~ with obtained said first password.

8. (Currently Amended) A storage medium data protecting apparatus for protecting data ~~on a storage medium~~, comprising:

a storage medium having a plurality of unit storage areas; and

a control circuit for reading and writing the data from and to said storage medium,

wherein said control circuit has:

a write mode of encrypting, after generating a random key ~~data~~, ~~the~~ said random key ~~data~~ with a password, writing the encrypted key ~~data~~ to said storage medium, encrypting the data with the random key ~~data~~, and writing the encrypted data to said storage medium;

a read mode of ~~encoding~~ decoding, after reading ~~the~~ said encrypted key ~~data~~ from said storage medium, the encrypted key ~~data~~ with ~~the~~ said password, and decoding the data on said storage medium with the decoded key ~~data~~,

wherein said write mode comprises a mode of generating a different random key ~~data~~ for each unit storage area of said ~~storage medium~~plurality of unit storage areas so that said each unit storage area is assigned a different random key, and the assignment of said different random key to said each unit storage area being based on a particular unit storage area to which the data, once encrypted, is to be stored, encrypting each ~~said~~ of the different random ~~key data for each unit storage area~~ keys with said password, writing each ~~said~~ of the encrypted ~~key data~~ keys to said storage medium when initializing the storage medium, and encrypting the data with the random key ~~data~~ corresponding to its said particular unit storage area to write the data,

wherein said read mode comprises a mode of decoding the data with the decoded key ~~data~~ corresponding to said particular unit storage area where the data have been read.

9. (Currently Amended) A storage medium data protecting apparatus according to claim 8, wherein said storage medium is constructed of a storage medium from and to which the data is read and written per logic sector,

and said control circuit generates ~~the~~ said different random key ~~data~~ per logic sector on said storage medium.

10. (Currently Amended) A storage medium data protecting apparatus according to claim 8, wherein said control circuit generates different ~~key data~~ random keys for each writing to said plurality of unit storage areas.

11. (Currently Amended) A storage medium data protecting apparatus according to claim 8, wherein said control circuit generates ~~the key data~~ said different random keys by combining a predetermined number of pieces of random data.

12. (Currently Amended) A storage medium data protecting apparatus according to claim 9, wherein said control circuit decodes, after reading ~~the~~ said encrypted key ~~data~~ from said storage medium, ~~the~~ said encrypted key ~~data~~ with an old password designated by a user, and writes, after encrypting ~~the~~ said decoded key ~~data~~ with a new password designated by the user, ~~the~~ said encrypted key ~~data~~ to said storage medium.

13. (Currently Amended) A storage medium data protecting apparatus according to claim 8, wherein said control circuit has:

a write mode of encrypting ~~the key data~~ said random keys with each of a plurality of passwords and writing the encrypted ~~key data~~ keys to said storage medium; and

a read mode of decoding the read/encrypted key ~~data~~ with ~~the~~ a designated password.

14. (Currently Amended) A storage medium data protecting apparatus according to claim 8, wherein said control circuit has:

a write mode of encrypting ~~the~~ said key ~~data~~ with a first password, writing ~~the~~ said encrypted key ~~data~~ to said storage medium, encrypting ~~a second~~said first password with ~~said first~~a second password, and writing ~~said second~~ the first encrypted password to said storage medium; and

a read mode of decoding said ~~second~~ first encrypted password with said second password, obtaining said first password, and thereafter decoding ~~the~~ said encrypted key ~~data~~ with said first password.

15. (Cancelled)

16. (Currently Amended) The storage medium protecting method according to claim 1, said writing ~~the~~ said encrypted key ~~data step~~ is performed for all unit storage areas of ~~said~~ the storage medium when initializing ~~said~~ the storage medium.

17. (Currently Amended) The storage medium protecting method according to claim 16, wherein said encrypting the data step comprises:

a step of reading ~~the~~ said encrypted key ~~data~~ from ~~said~~ the storage medium;

a step of decoding ~~said~~ the read encrypted key ~~data~~ with said password; and

a step of encrypting the data with ~~said~~ the decoded key ~~data~~.

18. (Currently Amended) An encoding method for protecting data on a storage medium having a plurality of unit storage areas, comprising:

a step of generating different random ~~key data~~ keys for each unit storage area of ~~said~~ the storage medium, encrypting ~~the~~ said different random ~~key data~~ keys with a password, and writing the encrypted ~~key data~~ keys to ~~said~~ the storage medium;

a step of encrypting the data with ~~the~~ a different random key ~~data~~ corresponding to ~~said~~ a particular unit storage area to which the data, once encrypted is to be written, and writing the encrypted data to ~~said~~ the storage medium.

19. (Currently Amended) A decoding ~~of protected~~ method for protecting data on a storage medium having a plurality of unit storage areas,

wherein different ~~key data is~~ keys are used for each unit storage area and the different ~~key data is~~ keys are encrypted with at least one password, comprising:

a step of reading the different encrypted ~~key data~~ keys from ~~said~~ the storage medium;

a step of decoding ~~the~~ said different encrypted ~~key data~~ keys with ~~said~~ the at least one password; and

a step of decoding the data on ~~said~~ the storage medium with ~~the~~ a particular decoded key ~~data~~ corresponding to ~~the~~ a particular unit storage area where the data, once encrypted have been read.

20. (Currently Amended) A storage medium data protecting method ~~of~~ for protecting data on a removable storage medium having a plurality of unit storage areas, comprising:

a step of generating random ~~key data~~ keys, encrypting said random ~~key data~~ keys with a password, and writing ~~said~~ the encrypted ~~key data~~ keys to the removable storage medium;

a step of encrypting the data on the removable storage medium with ~~said~~ the generated random ~~key data~~ keys, and writing ~~said~~ the encrypted data to the removable storage medium;

a step of reading said encrypted key ~~data~~ from the removable storage medium;

a step of decoding said encrypted key ~~data~~ with said password; and a step of decoding and reading the data on the removable storage medium with ~~said~~ the decoded encrypted key ~~data~~,

wherein said random key ~~data~~ generating step further comprises:

a step of generating different random ~~key data~~ keys for each ~~of a plurality of~~ unit storage ~~areas~~ area of the removable storage medium;

a step of encrypting each of said different random ~~key data~~ keys for said each ~~of said plurality of~~ unit storage ~~areas~~ area with said password; and

a step of writing each ~~said~~ of the encrypted ~~key data~~ keys to the removable storage medium,

wherein ~~said~~ the data encrypting step comprises a step of encrypting the data on the removable storage medium with a particular random key ~~data~~ corresponding to a ~~one of said plurality of~~ particular unit storage ~~areas~~ area to write the data, and

wherein ~~said~~ the data decoding step comprises a step of decoding the data on the removable storage medium with said decoded encrypted key ~~data~~ corresponding to ~~a one of said plurality of~~ said particular unit storage ~~areas~~ area where the data, once encrypted, have been read.

21. (New) A storage medium data protecting method of protecting data on a storage medium comprising:

a step of generating a random key, encrypting said random key with a password, and writing said encrypted random key to the storage medium;

a step of encrypting the data with the generated random key, and writing the encrypted data to the storage medium;

a step of reading said encrypted key from the storage medium;

a step of decoding said encrypted key with said password; and

a step of decoding the data on the storage medium with the decoded key,

wherein said writing said encrypted random key to the storage medium comprises a step of encrypting said random key with each of a plurality of passwords, writing said encrypted random keys to the storage medium, and said step of decoding the encrypted key comprises a step of decoding said encrypted key with a designated password.

22. (New) A storage medium data protecting method of protecting data on a storage medium comprising:

a step of generating a random key, encrypting said random key with a password, and writing said encrypted random key to the storage medium;

a step of encrypting the data with generated random key, and writing the encrypted data to the storage medium;

a step of reading said encrypted key from the storage medium;

a step of decoding said encrypted key with said password; and

a step of decoding the data on the storage medium with the decoded key, wherein said writing said encrypted random key to the storage medium comprises a step of encrypting said random key with a first password, writing the encrypted random key to the storage medium, encrypting said first password with a second password, and writing the encrypted first password to the storage medium, and

said step of decoding the encrypted key comprises a step of decoding said encrypted first password with said second password, and obtaining said first password, and a step of decoding said encrypted key with said obtained first password.

23. (New) A storage medium data protecting apparatus for protecting data, comprising:

a storage medium having a plurality of unit storage areas; and

a control circuit for reading and writing the data from and to said storage medium,

wherein said control circuit has:

a write mode of encrypting, after generating a random key, said random key with a password, writing said encrypted random key to the storage medium, encrypting the data with the generated random key, and writing the encrypted data to the storage medium; and a read mode of decoding, after reading said encrypted key from the storage medium, said encrypted key with said password, and decoding the data on the storage medium with the decoded key,

wherein said write mode has a mode of encrypting said random key with each of a plurality of passwords, writing said encrypted random keys to the storage medium, and

said read mode has a mode of decoding the encrypted key comprises a step of decoding said encrypted key with a designated password.

24. (New) A storage medium data protecting apparatus for protecting data, comprising:

a storage medium having a plurality of unit storage areas; and

a control circuit for reading and writing the data from and to said storage medium,

wherein said control circuit has:

a write mode of encrypting, after generating a random key, said random key with a password, writing said encrypted random key to the storage medium, encrypting the data with the generated random key, and writing the encrypted data to the storage medium; and

a read mode of decoding, after reading said encrypted key from the storage medium, said encrypted key with said password, and decoding the data on the storage medium with the decoded key, wherein said write mode has a mode of encrypting said random key with a first password, writing the encrypted random key to the storage medium, encrypting said first password with a second password, and writing the encrypted first password to the storage medium, and

said read mode has a mode of decoding said encrypted first password with said second password, and obtaining said first password, and a step of decoding said encrypted key with said obtained first password.

25. (New) A storage medium data protecting method of protecting data on a storage medium comprising:

a step of generating a random key, encrypting said random key with a password, and writing said encrypted random key to the storage medium;

a step of encrypting the data with the generated random key, and writing the encrypted data to the storage medium;

a step of reading said encrypted key from the storage medium;

a step of decoding said encrypted key with said password; and

a step of decoding the data on the storage medium with the decoded key,

wherein said writing encrypted key is performed for all unit storage areas of the storage medium when initializing the storage medium,

and wherein said encrypting the data step comprises:

a step of reading said encrypted key from the storage medium;

a step of decoding the read encrypted key with said password; and

a step of encrypting the data with the decoded key.

26. (New) A storage medium data protecting apparatus for protecting data, comprising:

a storage medium having a plurality of unit storage areas; and

a control circuit for reading and writing the data from and to said storage medium,

wherein said control circuit has:

a write mode of encrypting, after generating a random key, said random key with a password, writing said encrypted random key to the storage medium, encrypting the data with the generated random key, and writing the encrypted data to the storage medium; and

a read mode of decoding, after reading said encrypted key from the storage medium, said encrypted key with said password, and decoding the data on the storage medium with the decoded key,

and wherein said write mode has a mode of performing to write encrypted key for all unit storage areas of the storage medium when initializing the storage medium,

and wherein said write mode has a mode of reading said encrypted key from the storage medium, decoding the read encrypted key with said password, and encrypting the data with the decoded key.

27. (New) A storage medium data protecting method of protecting data on a storage medium comprising:

a step of generating a random key, encrypting said random key with a password, and writing said encrypted random key to the storage medium;

a step of encrypting the data with the generated random key, and writing the encrypted data to the storage medium;

a step of reading said encrypted key from the storage medium;

a step of decoding said encrypted key with said password; and

a step of decoding the data on the storage medium with the decoded key,

wherein further comprising:

a step of decoding, after reading said encrypted key from the storage medium, the said encrypted key with an old password designated by a user; and

a step of writing, after encrypting said decoded key with a new password designated by said user, the encrypted key to the storage medium.

28. (New) A storage medium data protecting apparatus for protecting data, comprising:

a storage medium having a plurality of unit storage areas; and

a control circuit for reading and writing the data from and to said storage medium, wherein said control circuit has:

a write mode of encrypting, after generating a random key, said random key with a password, writing said encrypted random key to the storage medium, encrypting the data with the generated random key, and writing the encrypted data to the storage medium; and

a read mode of decoding, after reading said encrypted  key from the storage medium, said encrypted key with said password, and decoding the data on the storage medium with the decoded key,

wherein said write mode further comprises a mode of decoding, after reading said encrypted key from the storage medium, the said encrypted key with an old password designated by a user, and writing, after encrypting said decoded key with a new password designated by said user, the encrypted key to the storage medium.